Performance Work Statement
Defense Manpower Data Center (DMDC)
Enterprise Information Technology Services II (EITS II)
DMDC Enterprise Initatives

1.0 INTRODUCTION

The Defense Manpower Data Center (DMDC) requires enterprise wide information technology services that can support the full range of IT services in order to develop, sustain and deliver new products, develop and maintain new IT systems, and design, deploy, and maintain the underlying infrastructure. The support will align IT resource expenditures with business goals and objectives and will enable an IT environment with innovative solutions that are responsive to organizational requirements.

2.0 BACKGROUND

DMDC has integrated new functionality in the Share point tool in the past year. In this PWS, these requirements are being driven by the need to sustain functionality of the enterprise Sharepoint tool. The tools that were developed or enhanced over the past year include eAdmin, eAgreements, eCorrespondence, and INEED.

3.0 SCOPE

The Contractor shall provide all necessary personnel and management required to support business tool automation sustainment.

4.0 REQUIREMENTS:

4.1 Provide Development and Sustainment Support for the automation of Business Tools

4.1.1 Sustain the DMDC and DHRA support tools in the Defense Information Systems Agency DOD Enterprise Portal Service(DISA DEPS) environment in order to effectively implement DHRA and DMDC streamlined processes.

4.1.2 Support the implementation of new processes in accordance with the DMDC business process reengineering initiatives. Develop and implement tools to automate or streamline new, DMDC approved business processes.

4.1.3 Ensure changes are recorded in a configuration management database and released software and documentation is archived in a software library in accordance with DMDC policy.

4.1.4 Prepare and execute milestone reviews for requirements, design, development and testing as required by the DMDC organization issuing the task order, to ensure the development meets the needs of the Government.

4.1.5 Provide industry best practices, practical assistance, and a high level of technical support, during and after implementation to ensure implementation is seamless and successful.

4.1.6 Coordinate testing and initial fielding of new software releases of business tools. Develop and monitor implementation schedule.

4.1.7 Distribute release notes and communication impact to customers for software releases to user acceptance, benchmark, stress test, and production regions.

4.1.8 Develop and maintain user manuals to support DMDC business tools in accordance with industry standards. The user manuals shall provide detailed instructions on how to use the DMDC business tools, where to obtain additional information, to ensure quick resolution of user issues and reduce help desk calls.

4.1.9 Develop quick reference guides for frequently executed workflows within DMDC business tools.

4.1.10 Provide user support for business tools to ensure timely resolution of user issues.

4.1.11 Provide transition support for business tools transitioning from DISA DEPS to other platforms (e.g. Task Management Tool (TMT), ServiceNow). Transition support includes providing functional and technical requirements details for DISA DEPS and supporting data transfer from DISA DEPS to other platforms.

4.2 KICK OFF MEETING

4.2.1 Participate in a Government scheduled Kick-off meeting within 5 calendar days of Task Order award. The purpose of this Kick-off meeting is to aid both the Government and Contractor personnel in achieving a clear and mutual understanding of all task requirements, and achievable deliverables within funding constraints; and identify and resolve potential problems. The Contractor shall be prepared to discuss any issues requiring clarification and gather information as necessary to support each deliverable. The contractor shall submit meeting minutes the DMDC PM and GSA COR NLT five (5) days after meeting completion.

4.3 Senior Management Review (SMR)

The Contractor shall follow the requirements identified in PWS Section 5.8.6 of the EITS II Base IDIQ.

4.4 Expenditure and Resource Report (ERR)

Provide an Expenditure and Resource Report (ERR) to the Government COR on a monthly basis. This report shall detail by PWS Task, each project that is being worked by the contractor, the amount that will be billed to the Government and the resources assigned to that task. Each report shall report on the previous month and provide the current month and cumulative task order costs by project.

4.5 QUALITY SURVEILLANCE

The Contractor shall follow the Quality Assurance requirements identified in the PWS Section 5.10 of the EITS II Base IDIQ.

4.6 Contract Discrepancy Report (CDR). In the event of unsatisfactory contractor performance, the DMDC PM or GSA COR or GSA CO will issue a CDR that will explain the circumstances and findings concerning the incomplete or unsatisfactory service. The contractor shall acknowledge receipt of the CDR and respond in writing as to how he/she shall correct the unacceptable performance and avoid a recurrence. The Government will review the contractor's corrective action response to determine acceptability and will use any completed CDR as part of an overall evaluation of Contractor performance when determining present or future contractual actions.

4.7 Problem Notification Reports (PNR).

The Contractor shall follow the PNR requirements identified in PWS Section 5.8.7 of the EITS II Base IDIQ.

5.0 Performance Standards

The incentive for achieving the Acceptable Quality Levels (AQLs) listed in the table below is a positive past performance evaluation, it should be understood that failure to meet the performance metrics below will result in negative past performance evaluations. All AQLs will be reported in the MSR.

Past Performance Evaluations will be submitted to the Contractor Performance Assessment Reporting System (CPARS) for all government agencies to review. Past Performance Evaluations will contain detailed narratives explaining reasons for positive and negative assessments. The following are the specific performance standards for this PWS. In addition to the below AQL table, the contractor shall meet all the requirements identified in Appendix D - SDLC - Process Handbook v2.0 of the EITS II IDIQ.

PERFORMANCE OBJECTIVE	PERFORMANCE THRESHOLD	METHOD OF SURVEILLANCE
Schedule: Deliverables are submitted on time.	No more than one (1) late deliverable per month. No deliverable late more than five (5) working days.	100% inspection

Business Relations: Proactive in identifying problems and recommending implementable solutions	Clear and consistent written or verbal responses and/or acknowledgement within one (1) working day of initial government notification.	100% inspection
Meet all Government and agency specific requirements	100% compliance	100% inspection to ensure that all Government and Agency specific requirements have been met. Independent verification of security procedures-defined by agency (could be performed by a third party or another agency according to current security regulations and measures).
Project Plan	100% of areas required by government including the WBS are created and updated monthly. On time delivery of Initial and Monthly Updates	100% Inspection

5.1 Reports, documents, and narrative type deliverables will be accepted when all discrepancies, errors, or other deficiencies identified in writing by the Government have been corrected. The general quality measures, set forth below, shall be applied to each deliverable received from the Contractor under this order:

- Accuracy – Deliverables shall be accurate in presentation, technical content, and adherence to accepted elements of style.
- Clarity – Deliverables shall be clear and concise; engineering terms shall be used, as appropriate. All diagrams shall be easy to understand, legible, and relevant to the supporting narrative. All acronyms shall be clearly and fully specified upon first use.
- Specifications Validity – All Deliverables must satisfy the requirements of the Government.
- File Editing – Where directed, all text and diagrammatic files shall be editable by the Government.
- Format – Deliverables shall follow DMDC guidance. Where none exists, the Contractor shall coordinate approval of format with the COTR.
- Timeliness – Deliverables shall be submitted on or before the due date specified

5.2 The Contractor's quality system shall demonstrate its prevention-based outlook by meeting the objectives stated in the PWS throughout all areas of performance and shall be developed to specify the Contractor's responsibility for management and quality control actions to meet the terms of the task order. The Contractor's QCP (PWS 4.4.1) shall be incorporated into and become part of this task order after the plan has been accepted by the Government. The Contractor's QCP shall be maintained throughout the life of the task order and shall include the Contractor's procedures to routinely evaluate the effectiveness of the plan to ensure the Contractor is meeting the performance standards and requirements of the contract.

5.3 The Contractor shall maintain a Lessons Learned document, updating it subsequent to each software release, disseminate and make recommendations to the Government to increase the quality of future deliverables and improve reliability and efficiency of systems. The Government will use a Quality Assurance Surveillance Plan (QASP) as part of the Government's efforts to monitor contractor performance.

6.0 DELIVERABLES

6.1 The Government will provide written acceptance, comments and/or change requests, if any, within 10 work days from Government receipt of the draft deliverable using the Deliverable Acceptance Checklist.

Deliverable	PWS Ref.	Due Date
Project Plan	4.1.1	30 days after award
Release notes	4.1.7	NLT production release
Business Tools User Manuals	4.1.8	NLT production release; updates within 10 business days of Government request
Business Tools Quick Reference Guides	4.1.9	NLT production release; updates within 10 business days of Government request
User Support Requests	4.1.10	Provide an initial response to all user support requests within 1 business day

7.0 GOVERNMENT FURNISHED PROPERTY/EQUIPMENT/INFORMATION (GFP/GFE/GFI)

7.1 Government Furnished Equipment (GFE) and Government Furnished Information (GFI) will be provided as necessary for the contractors located on site. Provided equipment will cover a broad spectrum to include office space, office equipment (desk, chairs, tables, cabinets, copiers, furniture, etc.), and IT/telecommunications equipment (computers, servers, peripherals, telephone systems, etc.)

7.2 The Government will provide all software code, in all forms and formats for the supported systems; system documentation, including architecture and design documents; complete database schemas and dictionaries; architecture and design documentation on services and APIs; training materials; current manuals; system and operational scripts; hardware; commercial off-the-shelf software; hosting facilities;

and all other relevant materials and equipment. The Government will facilitate and coordinate efforts with related Government entities required for system performance, operations, and support.

8.0 PLACE OF PERFORMANCE / HOURS OF OPERATION

8.1 The work under this task shall be performed on site at DMDC facilities in Seaside, CA. Any work performed at other locations must be identified in the formal submission and approved by the Government.

8.2 The contractor is responsible for conducting business between the hours of 8 a.m. to 5 p.m. ET, Monday thru Friday except Federal holidays or when the Government facility is closed due to local or national emergencies, administrative closings, or similar Government directed facility closings. The contractor must at all times maintain an adequate workforce for the uninterrupted performance of all tasks defined within this PWS when the Government facility is not closed for the above reasons. The work under this task may require off hours support during evening and weekend hours particularly for Tier 3 support and production implementations.

8.3 The Government may permit telecommuting by contractor employees when determined to be in the best interest of the Government in meeting work requirements. The contractor must have an established program subject to review by the Government. All telecommuting agreements must be authorized and approved by the COR and include the date, time, and description of the tasks to be performed. Telecommuting will be at no additional cost to the Government. Required travel to the Government site will be the expense of the contractor. The contractor shall provide adequate oversight of work products to ensure contract adherence. Contractors shall have formal telework policies in place if telework is employed. Telework arrangements on individual task order may commence with Contracting Officer and Contracting Officer Representative (COR) approval under the following:

- Telework requests shall be approved by the Contracting Officer and the Contracting Officer Representative.
- Any equipment provided by the Government for telework purposes will be treated as Government Furnished Equipment

9.0 PERIOD OF PERFORMANCE

The period of performance for this Task Order will be 12 months from date of award.

10.0 TRAVEL

10.1 The Government does not anticipate travel. The following applies if travel is necessary.

10.2 Local or long-distance travel may be required to various locations CONUS and OCONUS, as directed by the Government on a cost-reimbursable basis in accordance with the Joint Travel Regulations (JTR) Standardized Regulations per FAR 31.205-46, Travel Costs. All travel shall be coordinated in writing

through the DMDC Client Representative and travel must be pre-approved by the GSA CO (or their designated representative) prior to incurring costs.

10.3 All non-local travel must be pre-approved by the Government and must be in accordance with the applicable Government Travel Regulation.

10.4 Note: Specific travel destinations cannot be determined at this time. Travel will be performed at the direction of the Government on a not to exceed basis. Any unused travel amount for the current period of performance will NOT be carried over to the next period of performance. If travel costs are expected to exceed this amount, the contractor shall notify the Contracting Officer's Representative (COR) and obtain written authorization from the GSA Contracting Officer prior to travel.

10.5 Costs for transportation may be based upon mileage rates, actual costs incurred, or a combination thereof, provided the method used results in a reasonable charge. Travel costs will be considered reasonable and allowable only to the extent that they do not exceed on a daily basis, the maximum per diem rates in effect at the time of the travel.

11.0 SECURITY

11.1 The contractor shall comply with all security requirements detailed in the PWS of the EITS II BASE IDIQ.

11.2 In addition, all contractor personnel under this task order shall hold fully-adjudicated and active Secret security clearances. Contractor personnel shall possess these security clearances at Task Order award. In addition, personnel with access to CE production data must have a fully-adjudicated Single Scope Background Investigation (SSBI) and Security+ certification at time of award.

11.3 The Government requires the contractor to establish that applicants or incumbents either employed by the Government or working for the Government under this contract are suitable for the job and are eligible for a public trust position at the appropriate level at the start of the PoP date. This includes the following:

- US Citizen
- Favorable FBI fingerprint check
- Fully adjudicated background investigation completed

11.4 SECURITY CLEARANCE REQUIREMENTS

Contractor personnel must be able to obtain and maintain the requiring access to classified information will need to obtain the appropriate security clearance prior to beginning work on this contract.

11.4.1 DMDC is not responsible for processing contractor personnel for national security clearance (SECRET).

11.4.2 The contractor must comply with required DMDC personnel security requirements as specified by the Information Assurance Branch.

11.4.3 Interim Clearances will be reviewed upon notification to DMDC Information Security Branch.

11.4.4 It is the responsibility of the contractor FSO to notify DMDC immediately if there is a change in clearance eligibility.

11.4.5 If at any time, any Contractor FSO is unable to obtain/maintain an adjudicated Personnel Security Investigation (PSI), the contractor shall immediately notify the DMDC Information Assurance Branch and remove such person from work under this contract.

11.5 CAC REQUIREMENTS

11.5.1 Contractor personnel with access to DMDC systems or data must comply with HSPD-12 Personal Identity Verification (PIV) issuance requirements, known as the Common Access Card (CAC) for DMDC and must be CAC or PIV ready prior to beginning work on this contract:

11.5.2 All Contractor personnel must obtain/maintain a favorable FBI National Criminal History Check (fingerprint check).

11.5.3 Provide two forms of identity proofed identification (I-9 document).

11.5.4 Be citizens of the United States.

11.5.5 Submit a Standard Form (SF) 86 National Security Questionnaire through e-QIP that is favorably accepted by the Office of Personnel Management (OPM) for those:

- Who do NOT have an active security clearance
- Will be obtaining a position of trust through DMDC or
- Have NOT been favorably adjudicated within the last 24 months.

11.5.6 Schedule a Background investigation by OPM.

11.5.7 Maintain favorable FBI National Criminal History checks and ensure completion and successful adjudication as required for Federal employment.

11.5.8 Obtaining CAC or PIV ready status is the responsibility of the contractor. It is the responsibility of the contractor to notify DMDC when this is complete.

11.6 POSITION OF TRUST REQUIREMENTS

11.6.1 All contractor personnel with access to DMDC systems or data must comply with DODI 5200.2-R and DODI 8500.2. All persons on this contract will be designated as either an IT-I or IT-II as determined by the Government per position responsibilities.

11.6.2 Prior to beginning work on this contract, the contractor will complete all required DMDC personnel security requirements as specified by the Information Assurance Branch.

11.6.3 Submit a Standard Form (SF) 86 National Security Questionnaire through e-QIP that is favorably accepted by the Office of Personnel Management (OPM) for all employees under this contract requesting a position of trust.

11.6.4 It is the responsibility on the contractor to ensure their employees and sub-contractors (if applicable) comply with DMDC personnel security requirements.

11.7 LAN Access Requirements:

11.7.1 It is the responsibility of the contractor to comply with account access requirements as specified by the DMDC Information Assurance Branch. At minimum:

- Completed DMDC personnel security requirements.
- Complete DD 2875 Form(s) for all access required.
- Submit proof of completion for Personally Identifiable Information (PII) Training.
- Submit proof of completion Information Assurance/Cyber Awareness Challenge Training.
- Adhere to and sign the DMDC Information Systems User Agreement(s).

11.7.2 Information Assurance Requirements:

The contractor and all contractor personnel with access to or responsibility for nonpublic Government data under this contract shall comply with DoD Directive 8500.1 Information Assurance (IA), DoD Instruction 8500.2 Information Assurance (IA) Implementation, DoD Directive 5400.11 DoD Privacy Program, DoD 6025.18-R DoD Health Information Privacy Regulation, DoD 5200.2-R Personnel Security Program, and Homeland Security Presidential Directive (HSPD) 12.

11.7.3 The contractor shall establish appropriate administrative, technical, and physical safeguards to protect any and all nonpublic Government data to ensure the confidentiality, integrity, and availability of government data. At a minimum, this must include compliance with DoDD 8500.1 and DoDI 8500.2 and provisions for personnel security and the protection of sensitive information, including Personally Identifiable Information (PII).

11.7.4 Contractor systems and information networks that receive, transmit, store, or process nonpublic government data must be accredited according to DoDI 8510.01 DoD Information Assurance Certification and Accreditation Process (DIACAP) and comply with annual Federal Information Security Management Act (FISMA) security control testing. All systems subject to DIACAP must present evidence of Certification and Accreditation (C&A) testing in the form System Identification Profile (SIP), DIACAP Implementation Plan (DIP), DIACAP Scorecard and Plan of Action and Milestones (POA&M). Evidence of FISMA compliance must be presented in the form of a POA&M. The contractor will be responsible for the cost of IA C&A and FISMA testing required for any Contractor owned and operated network, facility and/or application processing DoD information.

11.7.5 The Contractor shall ensure all media containing sensitive information (e.g., hard drives, removable disk drives, CDs, DVDs) considered for disposal will be destroyed. Prior to destruction, media will be sanitized, i.e., all prudent and necessary measures shall be taken to ensure data cannot be retrieved through known conventional or unconventional means.

To the extent that the work under this contract requires the contractor to have access to DoD sensitive information the contractor shall after receipt thereof, treat such information as confidential and safeguard such information from unauthorized use and disclosure. The contractor agrees not to appropriate such information for its own use or to disclose such information to third parties unless specifically authorized by the Government in writing.

11.7.6 The contractor shall allow access only to those employees who need the sensitive information to perform services under this contract and agrees that sensitive information shall be used solely for the purpose of performing services under this contract. The contractor shall ensure that its employees will not discuss, divulge or disclose any such sensitive information to any person or entity except those persons within the contractor's organization directly concerned with the performance of the contract.

11.7.7 Contractor shall administer a monitoring process to ensure compliance with DoD Privacy Programs. Any discrepancies or issues should be discussed immediately with the Contracting Officer Representative (COR) and corrective actions will be implemented immediately.

11.7.8 The Contractor shall report immediately to the DMDC CIO / Privacy Office and secondly to the COR discovery of any Privacy breach. Protected PII is an individual's first name or first initial and last name in combination with any one or more of the following data elements: social security number; biometrics; date and place of birth; mother's maiden name; criminal, medical and financial records; educational transcripts, etc.

Government may terminate this contract for default if Contractor or an employee of the contractor fails to comply with the provisions of this clause. The Government may also exercise any other rights and remedies provided by law or this contract, including criminal and civil penalties.

11.7.9 The contractor shall be responsible for safeguarding all government equipment, information and property provided for contractor use. At the close of each work period, government facilities, equipment, and materials shall be secured.

12.0 INSPECTION, ACCEPTANCE AND PAYMENT

12.1 The Government will designate officials who have been delegated specific technical, functional and oversight responsibilities for this contract. The designated officials are responsible for inspection and acceptance of all services, incoming shipments, documents and services. The Contractor shall follow the Inspection and Acceptance requirements identified in the PWS Sections 7.0-7.5 of the EITS II Base IDIQ.

12.2 Delivery Address. All deliverables shall be submitted to the designated DMDC POC's. Additionally, if directed, the Contractor shall upload the deliverables into the GSA ITSS Portal.

12.3 Method of Delivery. The Contractor shall provide all deliverables and reports in the format of which to be defined or approved by the Government and subject to change over the course of the task order.

12.4 Acceptance Criteria. Acceptance by the Government of satisfactory services provided in contingent upon the Contractor performing in accordance with the performance standards contained in EITS Contract H98210-13-D-0003 and all terms and conditions of this Task Order, including all modifications.

12.5 Acceptance of Deliverables. The Government has 15 calendar days to review any draft documents and notify the contractor of approval or recommended changes to be made in the final version. If the Government does not provide an approval within the 15 days, the Contractor shall not assume that the deliverable is accepted by the Government. The contractor shall request a status update from the GSA COR. Final deliverables are then due within 10 working days after receipt of any Government comments on the draft. The Government COR has the final determination as to the format and the method that deliverables are submitted.

12.6 INVOICING

Requirements identified in the GSA Invoice Clause included in the EITS II Section B to E will be followed.

13.0 APPLICABLE DOCUMENTS

Document	Web link
DoD Instruction (DoDI) 8500.1, Cybersecurity	http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf
DoD 5200.2-R, Personnel Security Program	http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf